Presented to the Court by the foreman of the Grand Jury in open Court, in the presence of the Grand Jury and FILED in the U.S. DISTRICT COURT at Seattle, Washington.

November 15 20 17

WILLIAM M. McCOOL, Clerk

By _____ Deputy

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. MUHAMMAD FAHD, Defendant.	NO. CR17-290 RSL **INDICTMENT**

The Grand Jury charges that:

COUNT 1

(Conspiracy to Commit Wire Fraud)

I. INTRODUCTION

At all times material to this Indictment:

A. AT&T Mobility LLC

1. AT&T Mobility LLC (hereinafter, AT&T), was a company with headquarters in Atlanta, Georgia, and offices throughout the United States, including a customer service call center in Bothell, Washington.

2. AT&T sold cellular telephones and offered monthly voice and data plans for use with the phones on the AT&T wireless network. AT&T phones and wireless services were sold through authorized AT&T dealers and retailers across the country.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

3. AT&T offered subsidies to its customers by selling phones for less than the cost of the phones. AT&T recouped this subsidy investment through profits earned on the sale of AT&T wireless services by entering into service contracts with its customers.

4. Manufacturers that produced cellular telephones for AT&T installed proprietary locking software onto AT&T phones that prevented the phones from being used on any wireless network other than the AT&T network unless and until the phones were "unlocked."

5. "Unlocking" a phone disabled the proprietary locking software which allowed the phone to be used on multiple carrier systems rather than exclusively with AT&T.

6. The Wireless Customer Agreement between AT&T and each of its customers authorized AT&T to effectuate the unlocking of a customer's phone upon the satisfaction of certain criteria, such as when the customer had completed his or her contract or installment plan or paid off an installment plan early. Other circumstances in which AT&T might unlock a phone for a customer included when the customer wished to use the phone for international travel.

7. Unlocked phones were a valuable commodity because they could be resold and used on any other compatible networks around the world. When telephone customers switched to networks other than AT&T's network, the customers stopped paying AT&T for services, including, in some cases, before AT&T had recouped the costs of subsidies provided by AT&T on phones it had sold to the customers for less than the cost of the phones.

8. When a phone is unlocked fraudulently without AT&T's authorization, the fraudulent transaction deprives AT&T of its subsidy investment in the phone and the stream of payments on contracts that customers may no longer remit because they have switched service to another carrier.

9. AT&T employees at AT&T's Mobility Customer Care call center in Bothell, Washington, had access to AT&T's computer systems in order to assist AT&T

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

customers with service and billing issues. Among other things, AT&T employees at the call center had the ability to submit unlock requests on behalf of eligible customers.

10. AT&T employees used a variety of internal computer programs at AT&T to process unlock requests including, at times, a system called "Fat Albert," and a system called "Torch." Access to the systems was limited to authenticated users connected to AT&T's internal and protected corporate network.

11. AT&T's unlocking systems permitted AT&T employees with proper authorization and network credentials to, in appropriate circumstances, send requests to unlock the phones of AT&T customers.

B. Defendant

12. Defendant MUHAMMAD FAHD, was an individual living in Karachi, Pakistan, doing business as Endless Trading FZE, Endless Connections, Inc., and iDevelopment Co.

C. Definitions.

13. **Malware**: Malware was malicious computer code running on a computer that was not authorized by the owner/authorized user of that computer. Malware could be designed to do a variety of things, including logging every keystroke on a computer, stealing information or "user credentials" (passwords or usernames), and executing unauthorized commands on a computer without the consent of the authorized user.

II. THE OFFENSE

14. Beginning at a date uncertain, but no later than April 2012, and continuing through in or around September 2017, at Bothell, within the Western District of Washington, and elsewhere, defendant MUHAMMAD FAHD, aka Frank Zhang, and others known and unknown to the Grand Jury, did knowingly and intentionally, agree and conspire to devise and execute and attempt to execute, a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises; and in executing and attempting to execute this scheme and artifice, to knowingly cause to be transmitted in interstate and foreign

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

commerce, by means of wire communication, certain signs, signals and sounds as further described below, in violation of Title 18, United States Code, Section 1343.

III. THE OBJECT OF THE CONSPIRACY

15. The object of the conspiracy was to gain access to AT&T's protected internal computers without authorization, and in excess of authorization, by bribing AT&T employees to submit fraudulent and unauthorized cellphone unlocking requests through AT&T's internal protected computer network through, among other means, the installation of malware and unauthorized hardware on AT&T's internal network. The object further was to sell to members of the public the resulting ability to fraudulently unlock phones, so that the members of the public could stop using AT&T wireless services and deprive AT&T of its subsidy investment in customer cell phones and the value of the wireless service contracts it sold sell to members of the public.

IV. MANNER AND MEANS OF THE CONSPIRACY

A. Overview of the Conspiracy

16. It was part of the conspiracy that MUHAMMAD FAHD, and others known and unknown to the Grand Jury, gained unauthorized access to AT&T's internal protected computers through a variety of methods including by bribing AT&T employees (hereinafter "insiders") at AT&T's call center in Bothell, Washington, to use their network credentials and exceed their authorized access to AT&T's computers to submit large volumes of fraudulent and unauthorized unlock requests on behalf of the conspiracy and to install malware and unauthorized hardware on the AT&T systems.

17. From in or around April 2012, through in or around April 2013, MUHAMMAD FAHD, and others known and unknown to the Grand Jury, transmitted instructions to the insiders via the wires in interstate and foreign commerce, including lists of cellular telephone international mobile equipment identity (IMEI) numbers for the insiders to submit for fraudulent and unauthorized unlocking.

18. From in or around April 2013, through in or around October 2013, MUHAMMAD FAHD, and others known and unknown to the Grand Jury, also bribed

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

insiders to plant malware on AT&T's internal protected computers for the purpose of gathering confidential and proprietary information on how AT&T's computer network and software applications functioned.

19. Using information gathered by this malware about AT&T's computer network and software applications, MUHAMMAD FAHD, and others known and unknown to the Grand Jury, created additional malware designed to interact with AT&T's internal protected computers and automatically process fraudulent and unauthorized unlock requests submitted over the wires in interstate commerce from remote servers controlled by members of the conspiracy.

20. The malware MUHAMMAD FAHD, and others known and unknown to the Grand Jury, planted on AT&T's internal protected computers used network credentials that belonged to actual AT&T employees, including co-conspirators and others, to allow defendant, and others known and unknown to the Grand Jury, to log into AT&T's internal protected computers under false pretenses and automatically process fraudulent and unauthorized unlock requests.

21. From in or around November 2014, through in or around September 2017, MUHAMMAD FAHD, and others known and unknown to the Grand Jury, also bribed insiders to use their access to AT&T's physical work space to install unauthorized computer hardware devices including wireless access points designed to provide the conspiracy with unauthorized access to AT&T's internal protected computers and facilitate the automated process of submitting fraudulent and unauthorized unlock requests on behalf of the conspiracy.

22. The unauthorized computer hardware devices, like the malware, used network credentials that belonged to actual AT&T employees, including co-conspirators and others, to allow MUHAMMAD FAHD and others known and unknown to the Grand Jury to log into AT&T's internal protected computers under false pretenses and automatically process fraudulent and unauthorized unlock requests.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

B. Defendant Muhammad Fahd's Participation in the Conspiracy

23. It was part of the conspiracy that defendant MUHAMMAD FAHD, doing business as Endless Trading FZE (aka Endless Trading FZC), Endless Connections Inc., and iDevelopment Co. recruited insiders at AT&T who were willing to take bribes to work on behalf of the conspiracy.

24. MUHAMMAD FAHD contacted the insiders at AT&T via telephone, Facebook and other communication channels in interstate and foreign commerce and offered to pay them to unlock cell phones. MUHAMMAD FAHD instructed the insiders to obtain pre-paid cellular phones and anonymous online email accounts to continue communicating with him.

25. MUHAMMAD FAHD also instructed the insiders to create shell companies and open business banking accounts in order to receive payments for their work on behalf of the conspiracy.

26. MUHAMMAD FAHD obtained lists of IMEI numbers for cellular telephones from co-conspirators who offered unlocking services to customers for a fee.

27. Beginning in our around August 2012, MUHAMMAD FAHD sent lists of IMEI numbers for cellular telephones via the wires in interstate and foreign commerce to the insiders with instructions to submit unauthorized unlock requests for the IMEIs using their access to AT&T's protected internal computer network.

28. In or around April 2013, MUHAMMAD FAHD sent malware to the insiders via the wires in interstate and foreign commerce and instructed them to install the malware on AT&T's computer network. The malware was designed to gather confidential and proprietary information regarding the structure and functioning of AT&T's internal protected computers and applications.

29. Using information collected by the malware, MUHAMMAD FAHD, and others known and unknown to the Grand Jury, created additional malware (the "unlocking malware") designed to facilitate the transmission of commands via the wires

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

in interstate and foreign commerce from a remote server to AT&T's protected internal computer network and automatically submit unauthorized unlock requests.

30. MUHAMMAD FAHD sent the insiders multiple versions of the unlocking malware for purposes of testing and perfecting the malware on behalf of the conspiracy. Once the malware was perfected, MUHAMMAD FAHD instructed the insiders to plant the unlocking malware on AT&T's internal protected computers and run the unlocking malware while they were at work. The unlocking malware used valid AT&T network credentials that belonged to co-conspirators and others, without authorization, to interact with AT&T's internal protected computer network and process automated unauthorized unlock requests submitted from an external server.

31. In or around October 2013, AT&T discovered the unlocking malware and fired several insiders who were operating the unlocking malware at MUHAMMAD FAHD's direction.

32. In or around November 2014, MUHAMMAD FAHD recruited new insiders at AT&T willing to accept bribes to work on behalf of the conspiracy.

33. MUHAMMAD FAHD and others known and unknown to the Grand Jury, began programming hardware devices designed to facilitate unauthorized access to AT&T's internal protected network for the purpose of processing automated unauthorized unlock requests.

34. MUHAMMAD FAHD provided the hardware devices to co-conspirators including current and former AT&T insiders who tested the devices. Upon perfecting the operation of the devices, MUHAMMAD FAHD provided the devices to insiders who plugged the devices into AT&T's internal protected network without authorization to facilitate the unlocking of phones in furtherance of the conspiracy.

35. MUHAMMAD FAHD continued to pay insiders at AT&T to gain and maintain unauthorized access to AT&T's internal protected computer network, and exceed their authorized access to AT&T's protected internal computer network, plant malware, install unauthorized hardware, and operate malware and unauthorized hardware

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

on AT&T's protected internal computer network on behalf of the conspiracy through in or about September 2017.

All in violation of Title 18, United States Code, Section 1349.

COUNT 2

(Conspiracy to Commit Computer Fraud and Abuse Act and Travel Act Violations)

I. THE OFFENSE

36. The allegations set forth in Paragraphs 1 through 35 of Count 1 of this Indictment are re-alleged and incorporated as if fully set forth herein.

37. Beginning at a date uncertain, but no later than April 2012, and continuing through in or around September 2017, at Bothell, within the Western District of Washington, and elsewhere, defendant MUHAMMAD FAHD, aka Frank Zhang, and others known and unknown to the Grand Jury, did knowingly and intentionally agree and conspire to:

a. use a facility in interstate and foreign commerce, namely the wires, with the intent to promote, manage, establish, carry on and facilitate the promotion, management, establishment and carrying on of an unlawful activity, that is, Commercial Bribery in violation of the Revised Code of Washington Section 9A.68.060, and thereafter performed and attempted to perform an act to distribute the proceeds of such unlawful activity, and to promote, manage, establish and carry on, and to facilitate the promotion, management, establishment and carrying on of such unlawful activity in violation of Title 18, United States Code, Sections 1952(a)(1) and (3)

b. knowingly and with intent to defraud, access a protected computer without authorization and exceed authorized access to a protected computer, and by means of such conduct further the intended fraud and obtain anything of value exceeding $5,000.00 in any 1-year period, in violation of Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A); and

c. knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

authorization to a protected computer, and the offense caused loss to 1 or more persons during any 1-year period aggregating at least $5,000 in value and damage affecting 10 or more protected computers during a 1-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i).

II. THE OBJECT OF THE CONSPIRACY

38. The object of the conspiracy is set forth in Paragraph 15 of Count 1 of this Indictment and is re-alleged and incorporated as if fully set forth herein. Through this conduct, the conspiracy caused damages to AT&T's protected computers, including impairment to the integrity and availability of data, programs, systems, and information and caused losses to AT&T for the costs of responding to the offense, conducting damage assessments, restoring data, programs, systems and information and lost revenue during any 1-year period in excess of $5,000.00.

III. THE MANNER AND MEANS OF THE CONSPIRACY

39. The manner and means of the conspiracy are set forth in Paragraphs 16 through 35 of Count 1 of this Indictment and are re-alleged and incorporated as if fully set forth herein.

IV. Overt Acts

40. In furtherance of the conspiracy, and to achieve the objects thereof, defendant MUHAMMAD FAHD, and others known and unknown to the Grand Jury, did commit and cause to be committed, the following overt acts, within the Western District of Washington and elsewhere:

a. On or about April 9, 2012, Defendant MUHAMMAD FAHD opened a Google account with the email address unlockoutlet@gmail.com;

b. On or about April 13, 2012, co-conspirator 1 (CC-1) created account number 236199 with Softlayer, a cloud server hosting facility;

c. On or about August 1, 2012, MUHAMMAD FAHD opened a Facebook account in the name of "Frank Zhang";

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. In or around August 2012, MUHAMMAD FAHD recruited CC-2, an employee at AT&T in Bothell, Washington, to work in furtherance of the conspiracy using the wires in interstate and foreign commerce;

e. On or about August 2, 2012, CC-2 opened a Google account with the email address tyronejeromeskee@gmail.com;

f. On or about August 3, 2012, CC-1 sent a text message with the checking account number for CC-2 using the wires in interstate and foreign commerce;

g. On or about August 8, 2012, CC-1 wired a bribe payment in the amount of $4,000.00 to CC-2 from California to Marysville, Washington;

h. On or about August 30, 2012, CC-1 wired a bribe payment in the amount of $11,000.00 to CC-2 from California to Marysville, Washington;

i. On or about September 5, 2012, CC-2 sent an email from Bothell, in King County, Washington, to MUHAMMAD FAHD in Karachi, Pakistan, with the subject line "invoice number one" billing for "IT Services, client consulting, system architecture and infrastructure" and other computer related services;

j. In or around September 2012, CC-2 recruited CC-3, an employee at AT&T in Bothell, Washington on behalf of MUHAMMAD FAHD to work in furtherance of the conspiracy;

k. On or about September 20, 2012, CC-1 wired a bribe payment in the amount of $12,000.00 to CC-2 from California to Marysville, Washington;

l. On or about September 22, 2012, CC-3 opened a Google account with the email address yanghov687@gmail.com;

m. On or about October 11, 2012, CC-1 wired a bribe payment in the amount of $12,000.00 to CC-2 from California to Marysville, Washington;

n. On or about October 17, 2012, CC-3 provided MUHAMMAD FAHD with CC-3's bank account number and company name using the wires in interstate and foreign commerce;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

o. On or about October 20, 2012, MUHAMMAD FAHD instructed CC-1 to send money to CC-2 and CC-3 using the wires in interstate and foreign commerce;

p. On or about October 29, 2012, CC-1 wired a bribe payment in the amount of $10,000.00 to CC-3 from California to Des Moines, Washington;

q. On or about January 12, 2013, MUHAMMAD FAHD traveled to Dubai, United Arab Emirates from Karachi, Pakistan;

r. On or about January 19, 2013, CC-1 traveled to Dubai, United Arab Emirates from Los Angeles, California;

s. On or about January 22, 2013, MUHAMMAD FAHD met with CC-1 in Dubai, United Arab Emirates;

t. On or about April 11, 2013, MUHAMMAD FAHD opened a Yahoo account with the email address unlockoutlet@ymail.com;

u. On or about April 12, 2013, CC-3 opened a Yahoo account with the email address yanghov687@ymail.com;

v. In or around April 2013, MUHAMMAD FAHD provided CC-2 and CC-3, employees at AT&T in Bothell, Washington, with malware;

w. On or about April 11, 2013, CC-3 installed malware on AT&T's internal protected network;

x. On or about April 15, 2013, CC-1 wired a bribe payment in the amount of $11,000.00 to CC-2 from California to Marysville, Washington;

y. On or about April 15, 2013, CC-1 wired a bribe payment in the amount of $11,000.00 to CC-3 from California to Des Moines, Washington;

z. On or about April 20, 2013, CC-2 installed malware on AT&T's internal protected network;

aa. On or about April 30, 2013, CC-1 created account number 271319 with Softlayer, a cloud server hosting facility;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

bb. On or about May 13, 2013, CC-1 wired a bribe payment in the amount of $9,500.00 to CC-2 from California to Marysville, Washington;

cc. On or about May 15, 2013, CC-1 wired a bribe payment in the amount of $9,500.00 to CC-3 from California to Des Moines, Washington;

dd. On or about June 3, 2013, CC-1 wired $25,000.00 to MUHAMMAD FAHD in Karachi, Pakistan;

ee. On or about June 13, 2013, CC-1 wired a bribe payment in the amount of $8,500.00 to CC-2 from California to Marysville, Washington;

ff. On or about June 13, 2013, CC-1 wired a bribe payment in the amount of $8,500.00 to CC-3 from California to Des Moines, Washington;

gg. On or about July 31, 2013, CC-1 wired a bribe payment in the amount of $8,000.00 to CC-2 from California to Marysville, Washington;

hh. On or about July 31, 2013, CC-1 wired a bribe payment in the amount of $8,000.00 to CC-3 from California to Des Moines, Washington;

ii. In or around August 2013, CC-2 recruited CC-4, an employee at AT&T in Bothell, Washington, on behalf of MUHAMMAD FAHD to work in furtherance of the conspiracy;

jj. On or about August 23, 2013, CC-1 wired a bribe payment in the amount of $7,500.00 to CC-2 from California to Marysville, Washington;

kk. On or about August 23, 2013, CC-1 wired a bribe payment in the amount of $6,200.00 to CC-3 from California to Des Moines, Washington;

ll. In or around September 2013, CC-3 recruited CC-5, an employee at AT&T in Bothell, Washington, on behalf of MUHAMMAD FAHD to work in furtherance of the conspiracy;

mm. On or about September 23, 2013, CC-1 wired a bribe payment in the amount of $8,000.00 to CC-2 from California to Marysville, Washington;

nn. On or about September 23, 2013, CC-1 wired a bribe payment in the amount of $8,000.00 to CC-3 from California to Des Moines, Washington;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

oo. On or about September 27, 2013, CC-4 installed malware on AT&T's internal protected network;

pp. On or about September 30, 2013, CC-1 wired $68,000.00 to Endless Trading FZE, in Dubai, UAE;

qq. On or about October 18, 2013, CC-5 opened a Google account with the email address marvlewis691@gmail.com;

rr. On or about October 22, 2013, MUHAMMAD FAHD sent CC-5 instructions on how to operate malware on AT&T's internal protected network;

ss. On or about October 26, 2013, MUHAMMAD FAHD opened a Google account with the email address fahdibrahim85@gmail.com;

tt. On or about November 5, 2014, MUHAMMAD FAHD and CC-1 discussed accessing AT&T's internal protected network;

uu. On or about November 6, 2014, CC-2 opened a Google account with the email address paidinfullkid@gmail.com;

vv. On or about November 6, 2014, MUHAMMAD FAHD provided CC-1 with stolen network credentials for AT&T's internal protected network;

ww. On or about November 18, 2014, MUHAMMAD FAHD discussed programming routers to provide access to AT&T's internal protected network;

xx. On or about November 25, 2014, MUHAMMAD FAHD sent a router to CC-2 via FedEx from Dubai, UAE to Lynnwood, Washington;

yy. In or around November 2014, CC-2 provided a router configured to provide unauthorized access to AT&T's internal protected network to CC-5;

zz. On or about January 26, 2015, CC-1 wired $30,000 to Endless Trading FZE in Dubai, UAE;

aaa. On or about November 20, 2014, CC-6 wired $100,000.00 to Endless Trading FZE in Dubai, UAE;

bbb. On or about March 27, 2015, CC-1 wired $30,000.00 to Endless Trading FZE in Dubai, UAE;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ccc. On or about August 9, 2015, MUHAMMAD FAHD traveled to Dubai, United Arab Emirates, from Karachi, Pakistan;

ddd. On or about August 10, 2015, CC-2 traveled from Seattle, Washington to Dubai, UAE to pick up a bribe payment and meet with MUHAMMAD FAHD;

eee. On or about August 26, 2015, CC-1 wired $25,000.00 to Endless Trading FZE in Dubai, UAE;

fff. On or about December 5, 2015, AN traveled from Seattle, Washington to Houston, Texas to pick up a bribe for CC-5;

ggg. On or about December 16, 2016, MUHAMMAD FAHD opened a Google account with the email address fahd.patel85@gmail.com;

All in violation of Title 18, United States Code, Section 371.

COUNT 3

(Accessing a Protected Computer in Furtherance of Fraud)

1. The Grand Jury realleges and incorporates by reference the allegations in Counts 1 and 2 of this Indictment and further charges that:

2. Beginning at a date uncertain, but no later than in or around April 2013, and continuing until in or around October 2013, at Bothell, within the Western District of Washington and elsewhere, MUHAMMAD FAHD, and others known and unknown to the Grand Jury, knowingly and with intent to defraud accessed protected computers without authorization and exceeded authorized access and by means of such conduct furthered the intended fraud and obtained something of value, specifically, the defendant and others downloaded and installed malware onto AT&T's protected computers and executed the malware programs designed to facilitate fraudulent and unauthorized

///

///

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

unlocking transactions on AT&T's wireless network and by means of such conduct furthered the intended fraud and obtained things of value exceeding $5,000.00 in any 1-year period.

All in violation of Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A) and 2.

COUNT 4

(Intentional Damage to a Protected Computer)

1. The Grand Jury realleges and incorporates by reference the allegations in Counts 1 and 2 of this Indictment and further charges that:

2. Beginning at a date uncertain, but no later than in or around April 2013, and continuing until in or around October 2013, at Bothell, within the Western District of Washington and elsewhere, MUHAMMAD FAHD, and others known and unknown to the Grand Jury, knowingly caused the transmission of a program, information, code, and command, specifically malicious code that was downloaded and installed on AT&T's protected computers without AT&T's knowledge or consent, and as a result of such conduct, intentionally caused damage without authorization to protected computers, which damage caused losses to 1 or more persons during any 1-year period of at least $5,000.00 and affected 10 or more protected computers during a 1 year period.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i) and 2.

COUNT 5

(Accessing a Protected Computer in Furtherance of Fraud)

1. The Grand Jury realleges and incorporates by reference the allegations in Counts 1 and 2 of this Indictment and further charges that:

2. Beginning at a date uncertain, but no later than in or around November 2014, and continuing until in or around September 2017, at Bothell, within the Western District of Washington and elsewhere, MUHAMMAD FAHD, and others known and unknown to the Grand Jury, knowingly and with intent to defraud accessed protected

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

computers without authorization and exceeded authorized access and by means of such conduct furthered the intended fraud and obtained something of value, specifically, the defendant and others downloaded and installed malware onto AT&T's protected computers and executed the malware programs designed to facilitate fraudulent and unauthorized unlocking transactions on AT&T's wireless network and by means of such conduct furthered the intended fraud and obtained things of value exceeding $5,000.00 in any 1-year period.

All in violation of Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A) and 2.

COUNT 6
(Intentional Damage to a Protected Computer)

1. The Grand Jury realleges and incorporates by reference the allegations in Counts 1 and 2 of this Indictment and further charges that:

2. Beginning at a date uncertain, but no later than in or around November 2014, and continuing until in or around September 2017, at Bothell, within the Western District of Washington and elsewhere, MUHAMMAD FAHD, and others known and unknown to the Grand Jury, knowingly caused the transmission of a program, information, code, and command, specifically malicious code that was downloaded and installed on AT&T's protected computers without AT&T's knowledge or consent, and as a result of such conduct, intentionally caused damage without authorization to protected computers, which damage caused losses to 1 or more persons during any 1-year period of at least $5,000.00 and affected 10 or more protected computers during a 1 year period.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i) and 2.

FORFEITURE ALLEGATIONS

12. The allegations contained in Counts 1 through 6 of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Section 981(a)(1)(C), Title 28, United States

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Code, Section 2461(c), Title 18, United States Code, Section 982(a)(2)(B), and Title 18, United States Code, Section 1030(i) .

13. Pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), upon conviction of the offense in violation of Title 18, United States Code, Section 1349, as set forth in Count 1, the defendant shall forfeit to the United States of America, any property, real or personal, which constitutes or is derived from proceeds traceable to the charged offense. The property to be forfeited includes, but is not limited to, a sum of money representing the amount of proceeds the defendant obtained as a result of the charged offense.

14. Pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), upon conviction of a conspiracy to violate Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A) and Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i), in violation of Title 18, United States Code, Section 371, as set forth in Count 2, the defendant shall forfeit to the United States of America any property, real or personal, which constitutes or is derived from proceeds traceable to the charged offense. The property to be forfeited includes, but is not limited to, the following: a sum of money representing the amount of proceeds the defendant obtained as a result of the charged offense.

15. Pursuant to Title 18, United States Code, Section 982(a)(2)(B), and Title 18, United States Code, Section 1030(i) , upon conviction of a violation of Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A), as set forth in Counts 3 and 5, the defendant shall forfeit to the United States of America any property, real or personal, which constitutes or is derived from proceeds traceable to the charged offense. The property to be forfeited includes, but is not limited to, the following: a sum of money representing the amount of proceeds the defendant obtained as a result of the charged offense.

16. Pursuant to Title 18, United States Code, Section 982(a)(2)(B), and Title 18, United States Code, Section 1030(i) , upon conviction of a violation of Title 18,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i), as set forth in Counts 4 and 6, the defendant shall forfeit to the United States of America any property, real or personal, which constitutes or is derived from proceeds traceable to the charged offense. The property to be forfeited includes, but is not limited to, the following: a sum of money representing the amount of proceeds the defendant obtained as a result of the charged offense.

17. If any of the property described above, as a result of any act or omission of the defendants:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

///

///

///

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c).

A TRUE BILL:

DATED: 11.15.17

(Signature of Foreperson redacted pursuant to policy of the Judicial Conference)
FOREPERSON

ANNETTE L. HAYES
United States Attorney

ANDREW C. FRIEDMAN
Assistant United States Attorney

NORMAN BARBOSA
Assistant United States Attorney

FOR
ANDREW PAK
Trial Attorney
Computer Crimes and Intellectual Property Section

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970